UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/502,567	02/11/2000	Jorma Stenman	017.38045X00	5346

20457 7590 02/11/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/502,567	STENMAN ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *2/10/2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213..

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-17 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2402, 2367, 2407, 2401, and 2409 and Schneier "ISO Authentication Framework" p574-577

4. Henceforth, the examiner will refer the page numbers written into the actual RFC documents themselves, and not the page numbers appearing on the printouts. For example, page 2 of "The Internet Key Exchange" will begin where it reads "[Page 2]" to the right of "Standards Track"

The respective RFCs defining IKE, IPsec, IP Authentication Header, ESP, PF_Key Management API, and the embodying framework, ISAKMP are understood to be documents disclosing related

art and technologies, illustrating the groundwork for a subpart of a whole, specifically designed to be used with each other as part of an overall methodology for secure and reliable network communication.

For example:

- (RFC 2409 "The Internet Key Exchange (IKE)", page 2) discloses

  "This document describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF DOI."

- (RFC 2407 "The Internet IP Security Domain of Interpretation for ISAKMP", page 1) discloses

  "This document defines the Internet IP security DOI(IPsec DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations."

- (RFC 2367 "PF_Key Management", page 1) discloses

  "A generic key management API that can be used not only for IP Security [Atk95a] [Atk95b] [Atk95c] but also for other network security services is presented in this document. Version 1 of this API was implemented inside 4.4-Lite BSD as part of the U. S. Naval Research Laboratory's freely distributable and usable IPv6 and IPsec implementation[AMPMC96]."

- RFC 2401 "Security Architecture for the Internet Protocol", page 1) discloses

"1.3 Related Documents

As mentioned above, other documents provide detailed definitions of some of the components of IPsec and of their inter-relationship. They include RFCs on the following topics:

a. "IP Security Document Roadmap" [TDG97] -- a document providing guidelines for specifications describing encryption and authentication algorithms used in this system.

b. security protocols -- RFCs describing the Authentication Header (AH) [KA98a] and Encapsulating Security Payload (ESP) [KA98b] protocols.

c. algorithms for authentication and encryption -- a separate RFC for each algorithm.

d. automatic key management -- RFCs on "The Internet Key Exchange (IKE)" [HC98], "Internet Security Association and Key Management Protocol (ISAKMP)" [MSST97],"The OAKLEY Key Determination Protocol" [Orm97], and "The Internet IP Security Domain of Interpretation for ISAKMP" [Pip98]."

- RFC 2401 "Security Architecture for the Internet Protocol", page 7)

"The concept of a "Security Association" (SA) is fundamental to IPsec. Both AH and ESP make use of SAs and a major function of IKE is the establishment and maintenance of Security Associations."

It would have been obvious to one of ordinary skill in the art to combine RFC 2402, 2367, 2407, 2401, and 2409, because they are related protocols, designed to work together to allow for secure key exchanges, authentication, and network transmissions.

5. Henceforth the examiner will refer to the different documents describing the protocol framework as a single reference, describing a single system.

In reference to claim 1:

RFC 2402, 2367, 2407, 2401, and 2409 disclose all of claim 1 except,

- Applying the RFC 2402, 2367, 2407, 2401, and 2409 standards in a wireless local area network having a mobile terminal, access point, and a server, and associating the mobile terminal with the access terminal.
- Obtaining first and second certificates from a certificate authority and using them to generate the WLAN link level key and generate IPsec authentication.

The X.509 ISO Authentication Framework as disclosed in Schneier "Applied Cryptography" (p. 576-577 "Authentication Protocols") where **Alice is the mobile terminal, and Bob is the Access point** discloses using a certificate authority certificate, first certificate, and private key with Internet Key Exchange (IKE) to generate a WLAN link level key and mutually authenticating the mobile terminal and the access point using the IKE, where the first certificate is the certificate Alice gets when obtaining Bob's public key(paragraph 1, "Authentication Protocols"), the certificate authority certificate is Alice's certificate Ca that she sends to Bob(step 3, "Authentication Protocols"), and the private key signs the message (step 3, "Authentication Protocols"), and where the Alice, the mobile terminal, and Bob, the access point are authenticated having also established the WLAN link level keys.

The X.509 ISO Authentication Framework as disclosed in Schneier "Applied Cryptography" (p. 576-577 "Authentication Protocols") where **Alice is the mobile terminal, and Bob is the server** discloses using a certificate authority certificate, second certificate, and private key with Internet Key Exchange (IKE) to generate IPsec authentication encryption and decryption keys for data packets transferred between the mobile terminal and the server, where the second certificate is the certificate Alice gets from the CA to validate Bobs's certificate(paragraph 1, "Authentication Protocols"), the certificate authority certificate is the certificate Alice sends to Bob(step 3, "Authentication Protocols"), and the private key signs the message(step 3, "Authentication Protocols"), and where Alice the mobile terminal and Bob the server are IPsec authenticated.

The examiner takes official notice that it was well known in the art at the time of invention that wireless local area networks consisted of a mobile terminal, access point, a server, and associating the mobile terminal with the access point such as that described in Cyr et al. (US Patent 5,890,075), Raith (US Patent 5,237,612), or Lewis (US Patent 6,453,159).

The RFC 2402, 2367, 2407, 2401, and 2409 disclosed a series of network protocols designed to be used in any network that used IP. While a wireless network may use different a physical medium, it still used the IP protocol.

The X.509 ISO Authentication Framework's primary purpose was to provide authentication across networks while also establishing the keys for Public-Key Crytography.

It would have been obvious to one of ordinary skill in the art at the time of invention to:

- Apply RFC 2402, 2367, 2407, 2401, and 2409 in a WLAN because it would allow the same security advantages it gives to ground based networks to wireless networks, and it would allow easy integration and communication between networks and Certification Authorities since they would be using the same network standard.
- Apply the use of the X.509 ISO Authentication Framework because it would allow two parties to establish keys for communication and at the same time, authenticate both parties.

In reference to claim 2:

RFC 2402, 2367, 2407, 2401, and 2409 and Schneier "ISO Authentication Framework" p574-577 discloses a method wherein the certificate authority certificate, private key, and the first and second certificates are stored in the mobile terminal, where the CA certificate is Ca Alice sent to Bob the Access point, where the private key is Alice the mobile unit's private key, the first certificate is Bob the Access point's certificate(obtained from a CA), and where the second certificate is Bob the server's certificate(obtained from a CA).

In reference to claim 3:

It would have been obvious to one of ordinary skill in the art at the time of invention to store the certificate authority certificate, private key, and the first and second certificates in the mobile terminal at the time of creation to provide an initial secure key to allow for future cryptographic communications including changing the key in the future and avoid sending the initial key comprising its security and its subsequent encrypted and decrypted messages, should an eavesdropper be listening. The examiner notes Puhl et al. US patent 6223291 also discloses an example of this (Column 5, lines 58-61) & (Column 4, lines 54-65)

In reference to claim 4:

RFC 2401 discloses a method wherein the mobile terminal generates an authentication header for transferred data packets utilizing the IPsec encryption key. (RFC 2401, page 5, "How Ipsec works")

In reference to claim 5:

Schneier discloses a method, wherein the server authenticates and decrypts data packets transferred from the mobile terminal utilizing the IPsec authentication and decryption keys (Schneier, p. 576-577 "Authentication Protocols") where the IPsec authentication keys and decryption keys are the public and private keys established in the authentication protocol.

In reference to claim 6:

Schneier discloses a method wherein the data packets are transferred from the mobile terminal to the access point using WLAN link level encryption in addition to the IPsec encryption, (Schneier, p. 576-577 "Authentication Protocols") where the extra encryption is performed by the first set of keys established with the authentication protocol between the mobile terminal and the access point.

In reference to claim 7:

Schneier fails to disclose a method wherein the WLAN link level encryption comprises Wired Equivalent Privacy (WEP) encryption.

The examiner takes official notice that Wired Equivalent Privacy, WEP is a well known standard using the RC4 encryption algorithm in which the data is encrypted prior to being transmitted as defined in Section 8.2 "The Wired Equivalent Privacy Algorithm" of IEEE 802.11 1999 Edition and used by Lewis (Col 6, lines 53-57).

It would have been obvious to one of ordinary skill in the art at the time of invention to use WEP encryption in the WLAN link level encryption between the mobile terminal and the access point

because at the time of invention WEP was considered to be reasonably strong, efficient, and self synchronizing. (Section 8.2.2)

Claims 8-11 are rejected for the same reasons as claim 1.

In reference to claim 12:

RFC 2402("IP Authentication Header") discloses a method for use in a network in which MAC-level messages are transferred between a sender and receiver.

- generating an IPsec authentication header in a mobile terminal; RFC 2402 ("IP Authentication Header", page 1, paragraph 1), where the mobile terminal is the sender.
- including said IPsec authentication header in a MAC-level message transferred from the mobile terminal to an associated access point. RFC 2402 ("IP Authentication Header", page 1, paragraph 1) , where the associated access point is the receiver.

The RFC documents fail to explicitly disclose the use of Wireless Local Area Network (WLAN) as the physical implementation of these protocols, however it is understood that these protocols may be implemented in any network that uses IP.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement IKE, and consequently, the use of Authentication headers, and IPsec in a wireless network, all within the ISAKMP framework, because it would provide the same security of

network transmission to organizations with ground based networks, to those with wireless networks.

In reference to claim 13:

RFC 2367, "PF_Key Management API" discloses a generic key management API used for IPsec, or an IPsec kernel, where it is understood that in order to properly authenticate, this kernel or interface must be implemented by both parties, or in the case of a wireless network, through a mobile terminal and access point.

It is inherent that mobile terminals in wireless networks contain some kind of control process because the mobile terminal would need some method, system, or process, of negotiating the connection, controlling(by sending and receiving), and maintaining that connection with the rest of the wireless network.

In reference to claim 14:

RFC 2367, ("PF_Key Management API" a generic key management API used for IPsec, or an IPsec Kernel", page 41) discloses a method wherein the IPsec kernel builds the authentication header ("#define SADB_SATYPE_AH"), and where the authentication header would inherently be passed to the WLAN control process to have it sent to the other party involved in the authentication as the wireless network control process arbitrates the connection.

Claim 15 is rejected for the same reasons as claim 13.

In reference to claim 16:

RFC 2402, ("IP Authentication Header", Page 12) discloses a method wherein the WLAN control process determines that the MAC-level message contains IPsec authenticated data and extracts that data from MAC-level message, where the IPsec authenticated data is being transferred at MAC-level and the authenticated data is extracted by the receiver's WLAN control process(or process which controls the sending and receiving for the network) when it validates the messages, packets, and headers.

Claim 17 is rejected for the same reasons as claim 16.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

January 15th, 2003